ECI
IPSec Cryptographic Module
Version 1.6-FIPS-1

FIPS 140-2 Non-Proprietary
Security Policy

Level 2 Validation
Version 0.51

March 2004

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the IPSec Cryptographic Module from ECI Systems & Engineering (ECI). This security policy describes how the IPSec Cryptographic Module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The ECI website (http://www.ecimln.com) contains information on the full line of products from ECI.
- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to ECI. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to ECI and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact ECI.

ECI IPSEC CRYPTOGRAPHIC MODULE

Overview

The ECI IPSec Cryptographic Module is a software IPSec implementation that supports both IPSec and IKE functionality. The module provides IPSec services for use in securing communications between hosts and can be run on systems serving as clients, servers, or bridges. The module can be installed on machines used as workstations or servers.

The ECI Cryptographic Module is easily managed through a set of administration scripts, which allow an administrator to easily configure the module's IPSec functionality.

The ECI IPSec Cryptographic module uses Triple-DES to encrypt/decrypt IP traffic and HMAC with SHA-1 for integrity of IP traffic. Session keys are negotiated using IKE.

The ECI Cryptographic Module meets all relevant level 2 FIPS requirements when configured for a secure mode of operation.

Area	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security[1]	N/A
Operational Environment	2
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	NA

Table 1 – Validation Level

Module Interfaces

In FIPS 140-2 terms, the ECI Cryptographic Module is classified as a multi-chip standalone module. The module is capable of running on the Sun Solaris Operating System (OS) and must be run on the CC-certified EAL4 Trusted Solaris 8 4/01 for FIPS 140-2 purposes. (Details of how to configure this module for FIPS 140-2 can be found in the Secure Operation section of the document.)

The cryptographic boundary of the module is the case of the system, which physically encloses the complete set of hardware and software, including the all of the module's software components and the operating system.

[1] The module relies on the physical security of the host PC it runs on.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Logical Interface	Module Mapping	Physical Interface Mapping
Data Input Interface	Packet Interceptor - Streams interface to grab packets off the stack	RJ45 connector, RS232 connectors, Keyboard.
Data Output Interface	Packet Interceptor - Streams interface to insert packets into the stack	RJ45 connector, RS232 connector, Monitor port.
Control Input Interface	User Interface for ECI utilities and daemons	RJ45 connector, RS232 connectors, Keyboard.
Status Output Interface	User Interface for ECI utilities and daemons	RJ45 connector, RS232 connector, Monitor port.

Table 2 – FIPS 140-2 Logical Interfaces

Roles and Services

The module supports three roles: the Crypto-Officer, the User role, and the Remote Client User role. Operators assuming the Crypto-Officer and User roles are authenticated using identity-based authentication, while operators assuming the Remote Client User role are authenticated using role-based authentication.

Like the User role, the Remote Client User role uses the module to encrypt and decrypt data that is sent through the data input/output interfaces. But, the Remote Client User role is not authenticated by the OS, but rather, during IKE using preshared keys.

Crypto Officer Role

The Crypto-Officer role is responsible for initializing the module, initializing users and user passwords (operating system function), establishing user profiles (by running the ipsecadmin tool), and monitoring the use of the module (viewing log files periodically). Additionally, Crypto-Officers have access to the set of services provided to Users. Crypto-Officers are authenticated by the OS using a user ID (UID) and password.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Service	Description	CSP	Input	Output
Ipsecadmin	Script used to administrator the module: Starts/stops the policy manager View log files and status of policy manager Configure security policy database Create preshared keys	Preshared keys - write	Commands, configuration data	Result of commands
User administration	Create OS operators and operator passwords	Operator passwords – read/write	Commands and command line options, authentication data	Result of commands
Install	Install the module	SHA-1 HMAC key for software integrity check – write SHA-1 HMAC keys for bypass test –write	Commands and command line options	Result of commands
Uninstall	Uninstall the module and remove all files associated with the module	SHA-1 HMAC key for software integrity check - write SHA-1 HMAC keys for bypass test - write preshared keys - write	Commands and command line options	Result of commands
Zeroization	Reformat the hard drive(s) the module was installed on.	Preshared keys - write		

Service	Description	CSP	Input	Output
IPSec	Access the module's IPSec services	IPSec session keys (Triple-DES keys, SHA-1 HMAC keys) – read/write	IPSec inputs and data	IPSec outputs and data

Table 3 – Crypto Officer Services, Descriptions, CSPs

User Role

The User role uses the module to encrypt and decrypt data that is sent through the data input/output interfaces. The User does not have access to any of the module's applications or configuration files. Users are authenticated by the OS using a UID and password.

Descriptions of the services available to the User role are provided in the table below.

Service	Description	CSP	Input	Output
IPSec	Access the module's IPSec services		IPSec inputs and data	IPSec outputs and data
Password administration	Change their operator password	Operator password - write	Commands and command line options, authentication data	Result of commands

Table 4 – User Services, Descriptions, Inputs and Outputs

Remote Client User Role

Like the User role, the Remote Client User role uses the module to encrypt and decrypt data that is sent through the data input/output interfaces. But, the Remote Client User role is not authenticated by the OS, but rather, during IKE using preshared keys.

Descriptions of the services available to the User role are provided in the table below.

Service	Description	CSP	Input	Output
IPSec	Access the module's IPSec services		IPSec inputs and data	IPSec outputs and data

Table 5 – User Services, Descriptions, Inputs and Outputs

Authentication Mechanisms

The module implements password-based authentication and IKE preshared key-based authentication mechanisms.

Authentication Type	Strength
Preshared key-based authentication (IKE)	SHA-1 HMAC generation/verification is used to authenticate to the module during IKE with preshared keys. This mechanism is as strong as the HMAC with SHA-1 algorithm. Additionally, preshared keys must be at least 32 bytes long and are randomly generated using the module's FIPS-approved PRNG. Each byte can have 256 different combinations of bits, so the probability of randomly guessing the correct sequence is 1 in 256^32.
Password-based authentication	Passwords are required to be at least 6 characters in length. Numeric, alphabetic (upper and lower case), and keyboard/extended characters can be used, which gives a total of 95 characters to choose from. Considering only the case insensitive alphabet using a 6 digit password with repetition, the number of potential passwords is 26^6.

Table 6 – Estimated Strength of Authentication Mechanisms

Unauthenticated Services

Traffic that is not being processed by the module may be passed through the module without authentication. This traffic does not access any of the module's security functionality.

Physical Security

The ECI IPSec Cryptographic Module is a software module and does not implement any physical security mechanisms.

Cryptographic Key Management

The ECI IPSec Cryptographic Module implements the following FIPS-approved cryptographic algorithms:

- SHA-1 (Certificate #168) – as per FIPS PUB 180-1
- Triple-DES (Certificate #186) – as per FIPS PUB 46-3
- HMAC with SHA-1 (Certificate #168, vendor affirmed) – as per FIPS PUB 198

The module supports the following algorithms for the following uses in a FIPS-approved mode of operation:

- Pseudo Random Number Generation – as per ANSI X9.31 (formerly ANSI X9.17)

- Diffie-Hellman Key Agreement (used by IKE)

In addition, the EC100x supports the following protocols for use in a FIPS-approved mode of operation:

- IKE
- IPSec

Also, the module implements the following algorithms, which are not used in a FIPS-approved mode of operation:

- MD5
- HMAC with MD5
- RSA (PKCS #1)
- DSA
- CAST
- Blowfish

The ECI IPsec Cryptographic Module supports the following critical security parameters (CSPs):

Key	Key type	Generation	Storage	Use
Operator passwords	-	-	Stored on disk (/etc/password) - plaintext	User and Crypto-Officer authentication
Software/bypass integrity check key	SHA-1 HMAC keys (160 bit)	External to the module – hard-coded	Stored on disk (/usr/local/cots/ipsec/softintegrity) - plaintext	Integrity check of software
Preshared keys for IKE	IKE preshared key (256 bit)	FIPS-approved PRNG	Stored on disk – plaintext (/usr/local/cots/ipsec/ipseckeys/*.dat)	Authentication during IKE
Diffie-Hellman key pairs	Diffie-Hellman key pairs (768 bit)	Generated by IKE negotiations	RAM only (public parameters stored on disk) – plaintext (/usr/local/cots/ipsec/sshalgs.spd)	Key exchange during IKE

Encryption session keys for IPSec	TDES keys (64, 128, and 192 bit)	Generated by IKE negotiations	RAM only – plaintext	Encrypt/decrypt IPSec traffic
Authentication session keys for IPSec	SHA-1 HMAC keys (128 bit)	Generated by IKE negotiations	RAM only – plaintext	Authenticate IPSec traffic
X9.31 PRNG keys	Triple-DES (128 bit)	Generated by gathering entropy	RAM only – plaintext	Random number generator

Key Generation

Preshared keys are generated internally by the module using the FIPS-approved PRNG. Diffie-Hellman key pairs are generated internally by the module as need by IKE, and the FIPS-approved PRNG is used for the generation of these keys.

Key Establishment

Triple-DES and SHA-1 HMAC session keys are negotiated during IKE.

Key Entry and Output

All keys entered into or output from the module are done so electronically.

Key Storage

All of the module's keys, whether in volatile or non-volatile memory, are stored in plaintext form.

Key Zeroization

All keys on the module can be zeroized by reformatting the module's hard-drive. Session keys, Diffie-Hellman key pairs, and the X9.17 PRNG keys are all ephemeral keys stored only in the module's volatile memory and can be zeroized by rebooting the module. Additionally, dynamically allocated memory containing ephemeral keys is overwritten before it is freed.

Self-Tests

The module performs the following startup self-tests:

Cryptographic Algorithm Tests (on all implementations of FIPS-approved algorithms used by the module) - Known Answer Tests (KATs) are run at power-up for the Triple-DES encryption/decryption, SHA-1 hashing, HMAC calculation/verification, and the PRNG random data generation.

- Triple-DES KAT (kernel module and daemon) – The Triple-DES KAT takes known keys and a plaintext value, which is encrypted and compared to the expected ciphertext value. If the values differ, the test is failed. The Triple-DES KAT then reverses this process by taking a known ciphertext value and keys; performing decryption; and comparing the result to the known plaintext value. If the values differ, the test is failed. If they are the same, the test is passed.

- SHA-1 KAT (kernel module and daemon) - The SHA-1 performs a hashing KAT. The SHA-1 KAT takes a specific value and hashes it. This hash is then compared to the known hash. If the values differ, the test is failed. If they are the same, the test is passed.

- HMAC with SHA-1 KAT (kernel module and daemon) - The SHA-1 performs an HMAC KAT. The HMAC KAT takes a specific value and key and calculates an HMAC. This HMAC is then compared to the known HMAC. If the values differ, the test is failed. If they are the same, the test is passed.

- PRNG KAT (kernel module and daemon) - The module performs a PRNG KAT. Known keys, counter value, and seed are used to initialize the PRNG. A block of random data is then generated by the PRNG and compared to a stored value. If these values are the same, the test is passed. Otherwise, it is failed.

- Software Integrity Tests - The module checks the integrity of its software using an SHA-1 HMAC. If the HMAC verifies, the test is passed. Otherwise, it is failed.

- Bypass Mode Test -The module performs SHA-1 HMAC verification to ensure that policy files have not been modified.

- Diffie-Hellman KAT – The module performs a Diffie-Hellman key agreement using hard-coded values during startup and confirms that the shared secret agreed upon is equal to the known shared secret.

If a startup self-test fails, the module enters the error state, logs the error to the system log, and reboots.

The module performs the following conditional self-tests:

- Continuous Random Number Generator Test - This test is run upon generation of random data by the module's random number generators to detect failure to a constant value.

- Bypass Mode Test - The module performs SHA-1 HMAC verification to ensure that policy files have not been modified.

- Diffie-Hellman pairwise consistency check – The module performs a Diffie-Hellman key agreement using a newly generated key pair and confirms that the key pair is working properly.

If a conditional self-test fails, the module enters the error state, logs the error to the system log, and reboots.

Design Assurance

Microsoft Visual Source Safe (VSS) version 6.0 was used to provide configuration management for the module's source code and documentation. The features of VSS were utilized to provide access control and versioning for the module.

Mitigation of Other Attacks

The module is designed to meet the overall FIPS 140-2 level 2 requirements and provides the level of security that comes with meeting those requirements. The module does not provide any mitigation of special attacks.

SECURE OPERATION

The ECI IPSec Cryptographic Module meets level 2 FIPS 140-2 requirements when operated in the following manner.

The module must be installed on the CC-certified EAL4 Trusted Solaris 8 4/01 running on an Intel Pentium III processor (as required by the CC certification) . Details of this Operating System and how to configure it properly are contained in the Security Target produced for the CC certification.

Trusted Solaris user accounts must be configured with a minimum of 6 character passwords. This is the default setting in Solaris, and can be modified by editing the /etc/default/passwd file. Additionally, accounts must be configured with a maximum number (10) of failed login attempts (after which point the account is locked out).

The Crypto-Officer account has superuser privileges, and the User accounts can be any accounts with less privileges. But, the Crypto-Officer must change the permission of all of the module's binaries, scripts, configuration files, and key files to have permissions that allow read/write/execute access only to the Crypto-Officer.

For example, the following files compose the module's software:

- /usr/local/cots/ipsec/ipsecadmin
- /usr/local/cots/ipsec/script_tool
- /usr/kernel/drv/SSHipsec
- /usr/local/cots/ipsec/sshipm
- /usr/local/cots/ipsec/genkey
- /usr/local/cots/ipsec/setup_mln.s,
- /usr/local/cots/ipsec/setup_msu.sh
- /usr/local/cots/ipsec/setup_msw.sh
- /usr/local/cots/ipsec/keyadmin.sh
- /usr/local/cots/ipsec/create_mln.sh
- /usr/local/cots/ipsec/create_msu.sh
- /usr/local/cots/ipsec/create_msw.sh

- /usr/local/cots/ipsec/softintegrity
- /etc/rc2.d/S72ipsec

Additionally, the following files and locations contain the module's configurations:

- /usr/local/cots/ipsec/ipseckeys/*.dat
- /usr/local/cots/ipsec/sshalgs.spd
- /usr/local/cots/ipsec/softhash.dat
- /usr/local/cots/ipsec/sshipsec.spd

Crypto-Officer Guidance

The Crypto-Officer is responsible for installation and initialization of the module, configuration and management of the module, and removal of the module.

Installation

The module's installation media (CD-ROM) is contained in a shrink wrapped package, and ECI ships the media to the Crypto-Officer via standard carriers. The Crypto-Officer must examine the received package for tamper-evidence, including tears, scratches, and other irregularities.

The module's installation media does not provide access control. As such, the Crypto-Officer must maintain control of the installation media, especially after it has been removed from its shrink wrapped package.

Directions for installation of the module are contained with the installation media. Additional FIPS specific configuration instructions are detailed above.

Management

Once the module has been properly installed, it is managed using the ipsecadmin utility. The Crypto-Officer should only use this utility to manage the module and should not directly edit the module's configuration files. This utility provides the ability to start/stop the module, configure the policy file for IPSec, and generate preshared keys.

Besides configuring the module, the Crypto-Officer must monitor the status of the module. The Crypto-Officer should look at the system logs and the module's log files. If suspicious activity is found, the Crypto-Officer should take the module offline and investigate.

If the module consistently malfunctions or otherwise repeatedly enters an error state, the Crypto-Officer should contact ECI.

Termination

At the end of the life cycle of the module, the Crypto-Officer should reformat the hard drive containing the module's software. This will zeroize all keys and other CSPs.

User Guidance

The User access the module's VPN functionality through the use of the module's IPSec services. Although outside the boundary of the module, the User should be careful not to provide authentication information and session keys to other parties.

ACRONYMS

AH	Authentication Header
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IPSec	IP Security
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
SA	Security Association
SHA	Secure Hash Algorithm
VPN	Virtual Private Network
VSS	Visual Source Safe